J. Symbolic Computation (1987) **4**, 99–102

Computation of Integral Bases in Certain S_n Extensions of $\mathbb{Q}$

ECKART MAUS

Mathematisches Institut der Georg-August-Universität, Bunsenstraße 3/5, D-3400 Göttingen, F.R.G.

Let $E = \mathbb{Q}(\alpha)$ be an extension of degree n over $\mathbb{Q}$ such that the smallest Galois extension $L/\mathbb{Q}$ containing E has Galois group S_n. Conditions are given to ensure that $\mathbb{Z}[\alpha_1, \ldots, \alpha_n]$ is the ring of integers in L, where $\alpha_1, \ldots, \alpha_n$ are the conjugates of α. Examples are given by certain series of trinomial equations for α.

Introduction

Little is known about the arithmetic of non-solvable Galois extensions $L/\mathbb{Q}$. This comes partly from the fact that numerical examples are difficult to provide. Existing computer programs for integral bases, units and class numbers cannot be used because of the high degree and the huge discriminants of these extensions. Instead of a direct approach one may consider L as the Galois hull of an extension E of smallest degree n and develop the connection between the arithmetic of E and L. The arithmetic of E has been studied with this aim in mind for special series of non-solvable equations of degree $n = 5$ in Maus (1984) and numerical examples are fairly well accessible in general for, say, $n \leqslant 10$ and discriminants $\leqslant 10^6$ by computational methods (see, for instance, the forthcoming book by Pohst & Zassenhaus, 1987). Of course, L is completely determined by E, but in general it seems to be a highly non-trivial problem to derive the arithmetic of L from that of E. The purpose of this note is to exhibit such relations between integral bases of E and L for certain S_n-extensions. Our result is based on a simple discriminant formula and includes a result of Elstrodt *et al.* (1985). Examples are provided by the series of S_n extensions obtained by Uchida (1970), Yamamoto (1970), Osada (1987) and Maus (1984).

A Discriminant Formula

For a finite separable extension $N \supset M$ of fields the discriminant of a set

$$S = \{\beta_1, \ldots, \beta_m\} \subset N, m = (N : M)$$

is defined as

$$d_{N/M}(S) = \det (\mathrm{Tr}_{N/M} \beta_i \beta_j) = \det (\sigma_\nu \beta_j)^2,$$

where the σ_ν range over all distinct embeddings of N/M in a given algebraic closure of M.

Let F be a field and let f be an irreducible polynomial of degree $n \geqslant 2$ in $F[x]$ with the property that the decomposition field L of f is a Galois extension with Galois group S_n. Let $\alpha = \alpha_1, \ldots, \alpha_n$ be the roots of f in L and let $E = F(\alpha)$ and $D = d_{E/F}(1, \alpha, \ldots, \alpha^{n-1})$. It is

0747-7171/87/040099+04 $03.00/0

well known that D coincides with the discriminant

$$d(f) = \prod_{0<i<j\leqslant n} (\alpha_i - \alpha_j)^2$$

of f. Let

$$P = \{\alpha_1^{\nu_1} \ldots \alpha_n^{\nu_n} | 0 \leqslant \nu_i < n-i, i = 1, \ldots, n\}$$

be the product basis of L/F.

LEMMA. $d_{L/F}(P) = D^{\frac{n!}{2}}$.

PROOF. By induction on n (see Pohst & Zassenhaus, 1987, II.9, for example).

A Criterion for $O_L = \mathbb{Z}[\alpha_1, \ldots, \alpha_n]$

Let O_N denote the ring of integers in the algebraic number field N. The discriminant $\vartheta_{N/M}$ of N with respect to a subextension M is the ideal generated by all $d_{N/M}(S)$, where

$$S = \{\beta_1, \ldots, \beta_m\} \subset O_N,\ m = (N:M).$$

If $M = \mathbb{Q}$ and $\Omega = \{\omega_1, \ldots, \omega_n\}$ is an integral basis of N, i.e. $O_N = \mathbb{Z}[\omega_1, \ldots, \omega_n]$, then $d_{M/\mathbb{Q}}(\Omega)$ is called the discriminant d_N of N and we have $\vartheta_{N/\mathbb{Q}} = (d_M)$. The properties of discriminants we use here and in the following may be found in Hasse (1980).

Let

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0,\ a_i \in \mathbb{Z}$$

be an irreducible polynomial with the property that the decomposition field L of f has Galois group S_n. As above, let $\alpha = \alpha_1, \ldots, \alpha_n$ be the roots of f in L, $E = \mathbb{Q}(\alpha)$ and $D = d_{E/\mathbb{Q}}(1, \alpha, \ldots, \alpha^{n-1}) = d(f)$. The fixed field of $A_n \subset S_n$ is the quadratic field $K = \mathbb{Q}(\sqrt{D})$. The discriminant d_K of K differs from D at most by a square: $D = m^2 d_K$ with $m \in \mathbb{Z}$. In fact, let $D = e^2 D_0$, D_0 squarefree, $e \in \mathbb{Z}$. Then $d_K = 4D_0$ or D_0 according to whether $D_0 \equiv 2, 3$ or $\equiv 1 \bmod 4$. As a discriminant of algebraic integers D must be $\equiv 0$ or $1 \bmod 4$ by Stickelberger. Thus e must be even if $D_0 \equiv 2, 3 \bmod 4$.

THEOREM. *$D = d_K$ if and only if $O_L = \mathbb{Z}[\alpha_1, \ldots, \alpha_n]$ and L is unramified over K. The discriminant of L is then given by $d_L = D^{\frac{n!}{2}}$.*

PROOF. Let P be the product basis of the α_i as above. Then $\vartheta_{L/\mathbb{Q}} | d_{L/\mathbb{Q}}(P)$ and $\vartheta_{L/\mathbb{Q}} = (d_{L/\mathbb{Q}}(P))$ if and only if P is an integral basis of $L/\mathbb{Q}$. We use the transition formula for discriminants

$$\vartheta_{L/\mathbb{Q}} = N_{K/\mathbb{Q}}(\vartheta_{L/K}) \vartheta_{K/\mathbb{Q}}^{\frac{n!}{2}}.$$

If $D = d_K$ we get

$$\vartheta_{L/\mathbb{Q}} = N_{K/\mathbb{Q}}(\vartheta_{L/K}) . \left(D^{\frac{n!}{2}}\right) | d_{L/\mathbb{Q}}(P) = D^{\frac{n!}{2}},$$

which implies

$$\vartheta_{L/K} = (1) \quad \text{and} \quad \vartheta_{L/\mathbb{Q}} = \left(D^{\frac{n!}{2}}\right),$$

i.e. L/K is unramified and P is an integral basis of L. Conversely, if L/K is unramified and P is an integral basis of L, we get

$$\vartheta_{L/\mathbb{Q}} = \left(D^{\frac{n!}{2}}\right) = \vartheta_{K/\mathbb{Q}}^{\frac{n!}{2}} = \left(d_K^{\frac{n!}{2}}\right), \quad \text{i.e. } d_K = D.$$

COROLLARY 1. *If $D = d(f)$ is squarefree, then L/K is unramified and $O_L = \mathbb{Z}[\alpha_1, \ldots, \alpha_n]$.*

PROOF. As remarked above, D *is* $\equiv 0$ or 1 mod 4. If D is squarefree, then $D \equiv 1 \bmod 4$ and $d_K = D$.

REMARK. The result that L/K is unramified if $d(f)$ is squarefree has been proved in a different way by Elstrodt *et al.* (1985).

COROLLARY 2. *If $D = d_K$, then $O_E = \mathbb{Z}[\alpha]$ and L/K is unramified.*

As to the interesting converse of Corollary 2 we can only prove

COROLLARY 3. *Let $n < 6$ and $2 \nmid D$. If $O_E = \mathbb{Z}[\alpha]$ and L/K is unramified, then $D = d_K$ and consequently $O_L = \mathbb{Z}[\alpha_1, \ldots, \alpha_n]$.*

PROOF. $O_E = \mathbb{Z}[\alpha]$ implies $d_E = D$ and L/K unramified implies $\mathfrak{d}_{L/K} = (1)$. By the transition formula for discriminants applied to $L \supset E \supset \mathbb{Q}$ and $L \supset K \supset \mathbb{Q}$, we therefore get

$$(d_L) = \mathfrak{d}_{L/\mathbb{Q}} = N_{E/\mathbb{Q}}(\mathfrak{d}_{L/E})(D^{(n-1)!}) = \left(d_K^{\frac{n!}{2}}\right).$$

As we remarked above, $D = m^2 d_K$ and therefore

$$m^{(n-1)!2} \mid \frac{n!}{d_K^2} - (n-1)!$$

Now $D(=d_E)$ and d_K contain the same primes because L/K is unramified. Therefore our assumption $2 \nmid D$ implies that d_K is squarefree. Comparing exponents we see that

$$(n-1)!\,2 > \frac{n!}{2} - (n-1)!$$

for $n < 6$ and consequently m has to be 1 for $n < 6$.

In the spirit of our introduction we may combine these results as follows:

COROLLARY 4. *Let $n < 6$, $2 \nmid D$ and let L/K be unramified. Then the following statements are equivalent:*

$$(i)\ O_E = \mathbb{Z}[\alpha], \quad (ii)\ O_L = \mathbb{Z}[\alpha_1, \ldots, \alpha_n], \quad (iii)\ D \text{ is squarefree.}$$

EXAMPLES. Our results may be applied to trinomial equations $f(x) = x^n + ax^m + b$, which have been investigated by Uchida (1970), Yamamoto (1970), Osada (1987) and Maus (1984). The most general result obtained by Osada says that L has Galois group S_n and is unramified over K, if f is irreducible and if the coefficients a and b can be written as $a = a_0 c^n$, $b = b_0^m c^n$ with $(a_0 c(n-m)m, nb_0) = 1$. The discriminant of f is

$$d(f) = (-1)^{\frac{n(n-1)}{2}} b_0^{m(m-1)} c^{n(n-1)} d_0(f),$$

where

$$d_0(f) = n^n b_0^{(n-m)m} + (-1)^{n-1} m^m (n-m)^{n-m} a_0^n c^{nm}.$$

As a typical consequence from these and our results we mention:

Let $f(x) = x^n + ax + b$ be irreducible and $((n-1)a, nb) = 1$. Then Gal $(L/\mathbb{Q}) = S_n$, L/K is

unramified and $2 \nmid D = d(f)$. For $n < 6$ the following statements are equivalent:

(i) $O_E = \mathbb{Z}[\alpha]$, (iii) $D = d_K$,
(ii) $O_L = \mathbb{Z}[\alpha_1, \ldots, \alpha_n]$, (iv) D is squarefree.

References

Elstrodt, J., Grunewald, F., Mennicke, J. (1985). On unramified A_m-extensions of quadratic number fields. *Glasgow Math. J.* **27**, 31–37.

Hasse, H. (1980). *Number Theory*. Grundlehren der math. Wiss. 229. Berlin: Springer Verlag.

Maus, E. (1984). Zur Arithmetik einiger Serien nichtauflösbarer Gleichungen 5. Grades. *Abh. Math. Sem. Univ. Hamburg* **54**, 227–250.

Pohst, M., Zassenhaus, H. (1987). *Algorithmic Algebraic Number Theory*. Cambridge: Cambridge University Press.

Osada, H. (1987). The Galois group of the polynomial $x^n + ax^l + b$ (to appear).

Uchida, K. (1970). Unramified extensions of quadratic number fields II. *Tohoku Math. Jour.* **22**, 220–224.

Yamamoto, Y. (1970). On ramified Galois extensions of quadratic fields. *Osaka J. Math.* **7**, 57–76.